AMENDMENTS TO THE CLAIMS

Please add or amend the claims to read as follows and cancel without prejudice or disclaimer to resubmission in a divisional or continuation application claims indicated as cancelled:

1-29. (Canceled)

30. (New) A method of processing $GF(2^{2s})$ representation data, the method comprising converting $GF(2^{2s})$ representation data into corresponding $GF((2^s)^2)$ representation data by applying to said $GF(2^{2s})$ representation data a conversion operator related to a predetermined transformation.

31. (New) The method of claim 30, wherein said conversion operator is related to a representation-transformation matrix corresponding to said transformation.

32. (New) The method of claim 31, wherein said conversion operator comprises an inverse of said representation-transformation matrix.

33. (New) The method of claim 31, wherein said conversion operator comprises a combination of a linear transformation and said representation-transformation matrix.

34. (New) The method of claim 33, wherein said conversion operator comprises an inverse of a matrix product of said representation-transformation matrix and a parameter matrix.

35. (New) The method of claim 31, wherein said representation-transformation matrix is selected from a set of possible representation-transformation matrices based on a predetermined criterion.

36. (New) The method of claim 35, wherein each matrix of said set of matrices is defined by a root of an irreducible polynomial over said $GF(2^{2s})$ representation, and a field generator of the $GF((2^s)^2)$ representation.

37. (New) The method of claim 30, wherein said $GF((2^s)^2)$ representation is defined by an irreducible reduction polynomial over $GF(2^s)$ and an extension polynomial over $GF(2^s)$.

38. (New) The method of claim 37, wherein said extension polynomial over $GF(2^s)$ comprises an irreducible polynomial of a second degree over $GF(2^s)$.

39. (New) The method of claim 30, wherein said $GF(2^{2s})$ representation data comprises two or more data blocks, and wherein said method comprises processing said $GF((2^s)^2)$ representation data by performing on the two or more data blocks at least one operation in said $GF((2^s)^2)$ representation equivalent to at least one desired operation in said $GF(2^{2s})$ representation to provide processed $GF((2^s)^2)$ data.

40. (New) The method of claim 30 comprising processing said $GF((2^s)^2)$ representation data by performing at least one operation equivalent to at least one desired operation in said $GF(2^{2s})$ representation to provide processed $GF((2^s)^2)$ data.

41. (New) The method of claim 40, wherein said at least one desired operation comprises an inverse operation in said $GF(2^{2s})$ representation.

42. (New) The method of claim 40, wherein the at least one operation in said $GF((2^s)^2)$ representation comprises at least one operation selected from the group consisting of a squaring operation in said $GF((2^s)^2)$ representation, a multiplication operation in said $GF((2^s)^2)$ representation, a XORing operation in said $GF((2^s)^2)$ representation, and an inverse operation in said $GF((2^s)^2)$ representation.

43. (New) The method of claim 40 comprising converting said processed $GF((2^s)^2)$ data back into said $GF(2^{2s})$ representation by applying to said processed $GF((2^s)^2)$ data a de-conversion operator related to said predetermined transformation.

44. (New) The method of claim 43, wherein said conversion operator comprises a decryption conversion operator, and said at least one desired operation in said $GF(2^{2s})$ representation comprises at least one decryption operation in said $GF(2^{2s})$ representation.

45. (New) The method of claim 40, wherein said at least one desired operation in said GF(2^{2s}) representation comprises at least one encryption operation in said GF(2^{2s}) representation, and said de-conversion operator comprises an encryption de-conversion operator.

46. (New) The method of claim 30, wherein s equals four.

47. (New) The method of claim 30, wherein applying said conversion operator comprises applying one or more intermediate conversion operators to recursively convert said GF(2^{2s}) representation data into said GF($(2^s)^2$) representation data.

48. (New) A device for processing GF(2^{2s}) representation data, the device comprising:

an input conversion module to convert GF(2^{2s}) representation data into corresponding GF($(2^s)^2$) representation data;

an operations module to perform at least one operation in said GF($(2^s)^2$) representation equivalent to at least one desired operation in said GF(2^{2s}) representation to provide processed GF($(2^s)^2$) data; and

an output conversion module to convert said processed GF($(2^s)^2$) data back into said GF(2^{2s}) representation.

49. (New) The device of claim 48, wherein said input conversion module comprises a multiplier to multiply said GF(2^{2s}) data by a matrix related to a representation-transformation matrix corresponding to said transformation.

50. (New) The device of claim 48, wherein said input conversion module comprises a multiplier to multiply a linear transformation of said GF(2^{2s}) data by a matrix related to a representation-transformation matrix corresponding to said transformation.

51. (New) The device of claim 48, wherein said at least one desired operation comprises an inverse operation in said GF(2^{2s}) representation.

52. (New) The device of claim 48, wherein the at least one operation in said $GF((2^s)^2)$ representation comprises at least one operation selected from the group consisting of a squaring operation in said $GF((2^s)^2)$ representation, a multiplication operation in said $GF((2^s)^2)$ representation, a XORing operation in said $GF((2^s)^2)$ representation, and an inverse operation in said $GF((2^s)^2)$ representation.

53. (New) The device of claim 48, wherein said output conversion module comprises a multiplier to multiply said processed $GF((2^s)^2)$ data by a matrix related to a representation-transformation matrix corresponding to said transformation.

54. (New) The device of claim 48, wherein said output conversion module comprises a multiplier to multiply a linear transformation of said processed $GF((2^s)^2)$ data by a matrix related to a representation-transformation matrix corresponding to said transformation..

55. (New) The device of claim 48, wherein said $GF((2^s)^2)$ representation is defined by an irreducible reduction polynomial over $GF(2^s)$ and an extension polynomial over $GF(2^s)$.

56. (New) The device of claim 55, wherein said extension polynomial over $GF(2^s)$ comprises an irreducible polynomial of a second degree over $GF(2^s)$.

57. (New) The device of claim 48, wherein said at least one desired operation in said $GF(2^{2s})$ representation comprises at least one operation selected from the group consisting of a decryption operation in said $GF(2^{2s})$ representation, and an encryption operation in said $GF(2^{2s})$ representation.

58. (New) The device of claim 48, wherein s equals four.

59. (New) A method for determining a representation-transformation comprising:

synthesizing a plurality circuits corresponding to a plurality of representation-transformations from a $GF(2^{2s})$ representation into a $GF((2^s)^2)$ representation, respectively; and

selecting one of said plurality of representation-transformations based on at least one optimization criterion.

60. (New) The method of claim 59, wherein synthesizing said plurality of circuits comprises constructing said plurality of circuits.

61. (New) The method of claim 59, wherein synthesizing said plurality of circuits comprises simulating said plurality of circuits.

62. (New) The method of claim 59, wherein s equals four.

63. (New) The method of claim 59, wherein said at least one criterion comprises a criterion selected from the group consisting of circuit area and power consumption.

64. (New) An encryption/decryption device for encrypting/decrypting $GF(2^{2s})$ representation data, the device comprising:

an input conversion module to convert data in a $GF(2^{2s})$ representation into corresponding data in a $GF((2^s)^2)$ representation, said input conversion module comprising decryption conversion circuitry and encryption conversion circuitry;

an operations module to perform on an output of said input conversion module at least one operation equivalent to a desired encryption/decryption operation in said $GF(2^{2s})$ representation to provide processed $GF((2^s)^2)$ data; and

an output de-conversion module to convert said processed $GF((2^s)^2)$ data back into said $GF(2^{2s})$ representation, said output conversion module comprising decryption de-conversion circuitry and encryption de-conversion circuitry.

65. (New) The device of claim 64, wherein said encryption conversion circuitry comprises a multiplier to multiply said $GF(2^{2s})$ data by an inverse of a representation-transformation matrix corresponding to related to a predetermined transformation.

66. (New) The device of claim 64, wherein said decryption conversion circuitry comprises:

an adder to add a cipher parameter vector to said $GF(2^{2s})$ data; and

a multiplier to multiply an output of said adder by an inverse of a multiplication of a cipher parameter matrix and a representation-transformation matrix corresponding to a predetermined transformation.

67. (New) The device of claim 64, wherein said at least one desired operation comprises an inverse operation in said $GF(2^{2s})$ representation.

68. (New) The device of claim 64, wherein the at least one operation in said $GF((2^s)^2)$ representation comprises at least one operation selected from the group consisting of a squaring operation in said $GF((2^s)^2)$ representation, a multiplication operation in said $GF((2^s)^2)$ representation, a XORing operation in said $GF((2^s)^2)$ representation, and an inverse operation in said $GF((2^s)^2)$ representation.

69. (New) The device of claim 64, wherein said decryption de-conversion circuitry comprises a multiplier to multiply said processed $GF((2^s)^2)$ data by a matrix related to a representation-transformation matrix corresponding to a predetermined transformation.

70. (New) The device of claim 64, wherein said encryption de-conversion circuitry comprises:

a multiplier to multiply said processed $GF((2^s)^2)$ data by a multiplication of a cipher parameter matrix and a representation-transformation matrix corresponding to a predetermined transformation; and

an adder to add a cipher parameter vector to an output of said multiplier.